



Department of Defense **DIRECTIVE**

December 13, 1996
NUMBER 5200.1

ASD(C31)

SUBJECT : DoD Information Security Program

References : (a) DoD Directive 5200.1, subject as above, June 7, 1982 (hereby canceled)
(b) Executive Order 12958, "Classified National Security Information, " April 20, 1995, as amended
(c) Information Security Oversight Office Directive, "Classified National Security Information, " October 13, 1995
(d) DoD Instruction 5230.21, "Protection of Classified National Security Council and Intelligence Information, " March 15, 1982 (hereby canceled)
(e) through (i) , see enclosure 1

A. REISSUANCE AND PURPOSE

This Directive:

1. Reissues reference (a) to update policy and responsibilities for the DoD Information Security Program under references (b) and (c).
2. Replaces references (d) through (f) .
3. Continues to authorize the publication of DoD 5200. 1-R (reference (g)), in accordance with DoD 5025.1-M (reference (h)) .

B. APPLICABILITY

This Directive applies to the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Inspector General of the Department of Defense, the Defense Agencies, and the DoD Field Activities (hereafter referred to collectively as "the DoD Components") .

C. DEFINITIONS

1. Compromise. A communication or physical transfer of classified information to an unauthorized recipient.

2. Information. Any knowledge that may be communicated or documentary material, regardless of its physical form or characteristics, that is owned by, produced by or for, or is under the control of, the Department of Defense.

3. National Security. The national defense or foreign relations of the United States.

D. Policy

It is DoD policy that:

1. National security information shall be classified, declassified and safeguarded, in accordance with national-level policy issuances. Misclassification shall be avoided.

2. Declassification of information shall receive equal attention with classification to ensure that information remains classified only as long as required by national security considerations .

3. The volume of classified national security information shall be reduced to the minimum necessary to meet operational requirements.

4. An active security education and training program shall be established and maintained to ensure that DoD military and civilian personnel who require access to classified national security information in the conduct of official business are familiar with their responsibilities for protecting such information from unauthorized disclosure.

E. RESPONSIBILITIES

1. The Assistant Secretary of Defense for Command, Control, Communications, and Intelligence shall:

a. Serve as the Senior Agency Official for the Department of Defense under subsection 5.6. (c) of E.O. 12958, as amended (reference (b)).

b. Direct, administer, and oversee the DoD Information Security **Program** to ensure that the program is efficient, recognizes assigned authorities and responsibilities, and that appropriate management safeguards are in place to prevent fraud, waste, and abuse.

c. Approve, when appropriate, requests for exceptions to DoD Information Security Program **policies** and procedures.

d. Approve and publish DoD Instructions and Publications,

as necessary, to guide, direct, or help DoD Information Security Program activities, consistent with DoD 5025.1-M (reference (h)) .

e. Encourage liaison between the DoD Components and industry; professional associations; academia; Federal, State, and local government organizations; and international organizations to acquire information that may be of use in improving the DoD Information Security Program.

f. Assist the Under Secretary of Defense for Acquisition and Technology, as required, in implementing the DoD Acquisition Systems Protection Program, both by establishing security policy and providing technical security support to that program.

2. The Under Secretary of Defense for Policy shall:

a. Direct, administer and oversee that portion of the DoD Information Security Program pertaining to Special Access Programs, foreign government (including North Atlantic Treaty Organization) classified information, the National Disclosure Policy and security arrangements for international programs.

b. Approve, when appropriate, requests for exception to policy involving any programs listed in paragraph E.2.a., above.

3. The Assistant Secretary of Defense for Public Affairs shall:

a. Direct and administer a DoD Mandatory Declassification Review Program under subsection 3.6. of E.O. 12958 (reference (b)) .

b. Establish policies and procedures for processing mandatory declassification review requests, including appeals consistent with subsection 3.6. (d) of reference (b) and Section 2001.13 of the Information Security Oversight Office Directive (reference (c)), which make maximum use of DoD Component resources and systems established to implement DoD Directive 5400.7 (reference (i)).

4. The Under Secretary of Defense for Acquisition and Technology shall serve as the office of primary responsibility and provide day-to-day direction and management of the DoD Acquisition Systems Protection Program.

5. The Secretaries of the Military Departments, as Agency Heads under reference (b), and the Heads of the Other DoD Components, shall:

a. Designate a senior agency official for their respective Departments who shall be responsible for the direction and

administration of the Department's information security program, to include active oversight, classification, declassification and security education and training programs to ensure effective implementation of reference (b) and DoD 5200.1-R (reference (g)) .

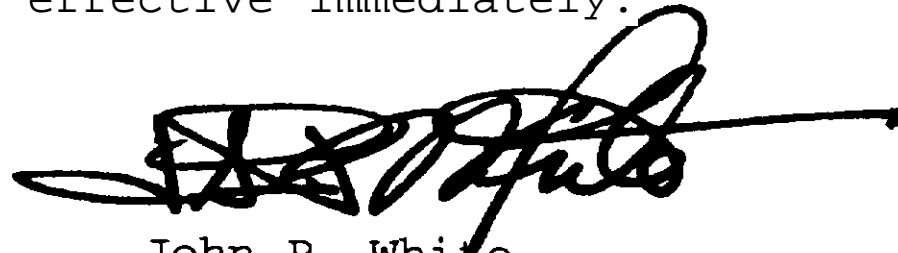
b. Ensure that funding and resources are adequate to carry out such oversight, classification, declassification and security education and training programs.

c. Consider and take action on complaints and suggestions from persons in or outside the Government regarding the Department's Information Security Program.

6. The Director, National Security Agency, shall, as the designee of the Secretary of Defense, when necessary, impose special requirements on the classification, declassification, marking, reproduction, distribution, accounting, and protection of and access to classified cryptologic information.

F. EFFECTIVE DATE

This Directive is effective immediately.

A handwritten signature in black ink, appearing to read 'John P. White', with a long horizontal stroke extending to the right.

John P. White
Deputy Secretary of Defense

Enclosure
References

REFERENCES, continued

- (e) DoD Instruction 0-5230.22, "Security Controls on the Dissemination of Intelligence Information, " August 17, 1988 (hereby canceled)
- (f) DoD Directive 5200.12, "Conduct of Classified Meetings, " July 27, 1992 (hereby canceled)
- (g) DoD 5200.1-R, "Department of Defense Information Security Program Regulation, " January 17, 1997 authorized by this Directive
- (h) DoD 5025.1-M, "DoD Directives System Procedures, " August 1994, authorized by DoD Directive 5025.1, June 24, 1994
- (i) DoD Directive 5400.7, "DoD Freedom of Information Act Program, " May 13, 1988